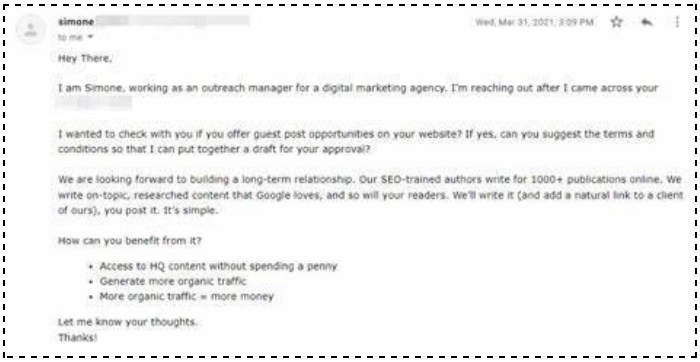
Notes (02/12/2024)

Here we have 5 cases of spam emails that look like phishing scams, below each image is why I think so.

Case 1:



simone
to me
Wed, Mar 31, 2021, 3:09 PM

Hey There,

I am Simone, working as an outreach manager for a digital marketing agency. I'm reaching out after I came across your

I wanted to check with you if you offer guest post opportunities on your website? If yes, can you suggest the terms and conditions so that I can put together a draft for your approval?

We are looking forward to building a long-term relationship. Our SEO-trained authors write for 1000+ publications online. We write on-topic, researched content that Google loves, and so will your readers. We'll write it (and add a natural link to a client of ours), you post it. It's simple.

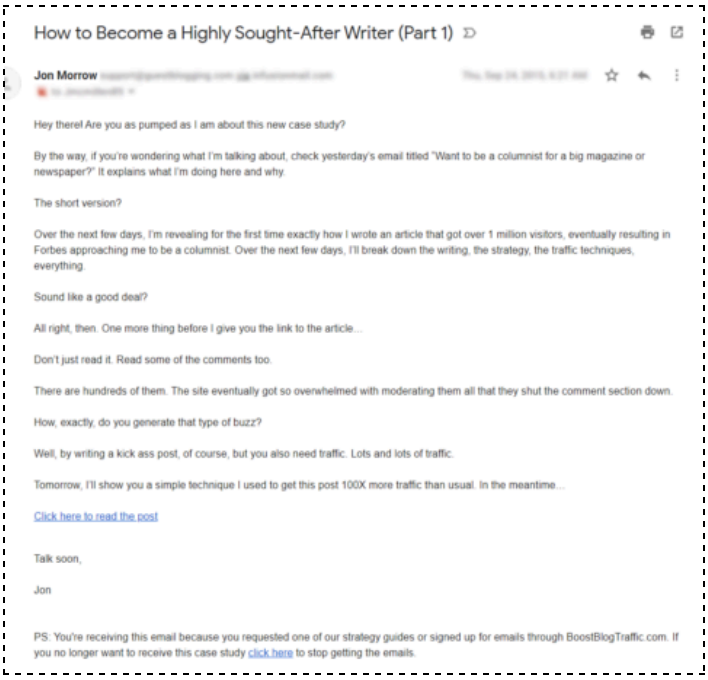
How can you benefit from it?

- Access to HQ content without spending a penny
- Generate more organic traffic
- More organic traffic = more money

Let me know your thoughts.
Thanks!

1. **Unsolicited Outreach:** The email appears to be unsolicited, meaning the recipient did not initiate contact with the sender. Phishing emails often arrive unexpectedly.
2. **Generic Greeting:** The email lacks a personalized greeting. Instead, it opens with a generic introduction ("I'm reaching out as an outreach manager..."). Legitimate communications usually address recipients by name.
3. **Too Good to Be True:** The sender offers to write content for free, emphasizing benefits like increased organic traffic and revenue. This overly positive tone can be a red flag.
4. **Urgency or Pressure:** The email doesn't explicitly pressure the recipient, but it implies that they should act promptly to take advantage of the offer ("Looking forward to your thoughts"). Phishing emails often create a sense of urgency.
5. **Suspicious Links:** Although there are no visible links in the snippet, phishing emails often include links that lead to malicious websites. These links may appear legitimate but actually direct users to fake login pages or malware-infected sites.
6. **Request for Sensitive Information:** While not explicitly stated, the sender may eventually ask for personal or website login details. Phishing emails often aim to steal sensitive information.
7. **Unusual Sender:** The sender claims to be an "outreach manager" from a digital marketing agency. However, the recipient may not have any prior relationship with this agency.

Case 2:



How to Become a Highly Sought-After Writer (Part 1)

Jon Morrow

Hey there! Are you as pumped as I am about this new case study?

By the way, if you're wondering what I'm talking about, check yesterday's email titled "Want to be a columnist for a big magazine or newspaper?" It explains what I'm doing here and why.

The short version?

Over the next few days, I'm revealing for the first time exactly how I wrote an article that got over 1 million visitors, eventually resulting in Forbes approaching me to be a columnist. Over the next few days, I'll break down the writing, the strategy, the traffic techniques, everything.

Sound like a good deal?

All right, then. One more thing before I give you the link to the article...

Don't just read it. Read some of the comments too.

There are hundreds of them. The site eventually got so overwhelmed with moderating them all that they shut the comment section down.

How, exactly, do you generate that type of buzz?

Well, by writing a kick ass post, of course, but you also need traffic. Lots and lots of traffic.

Tomorrow, I'll show you a simple technique I used to get this post 100X more traffic than usual. In the meantime...

Click here to read the post

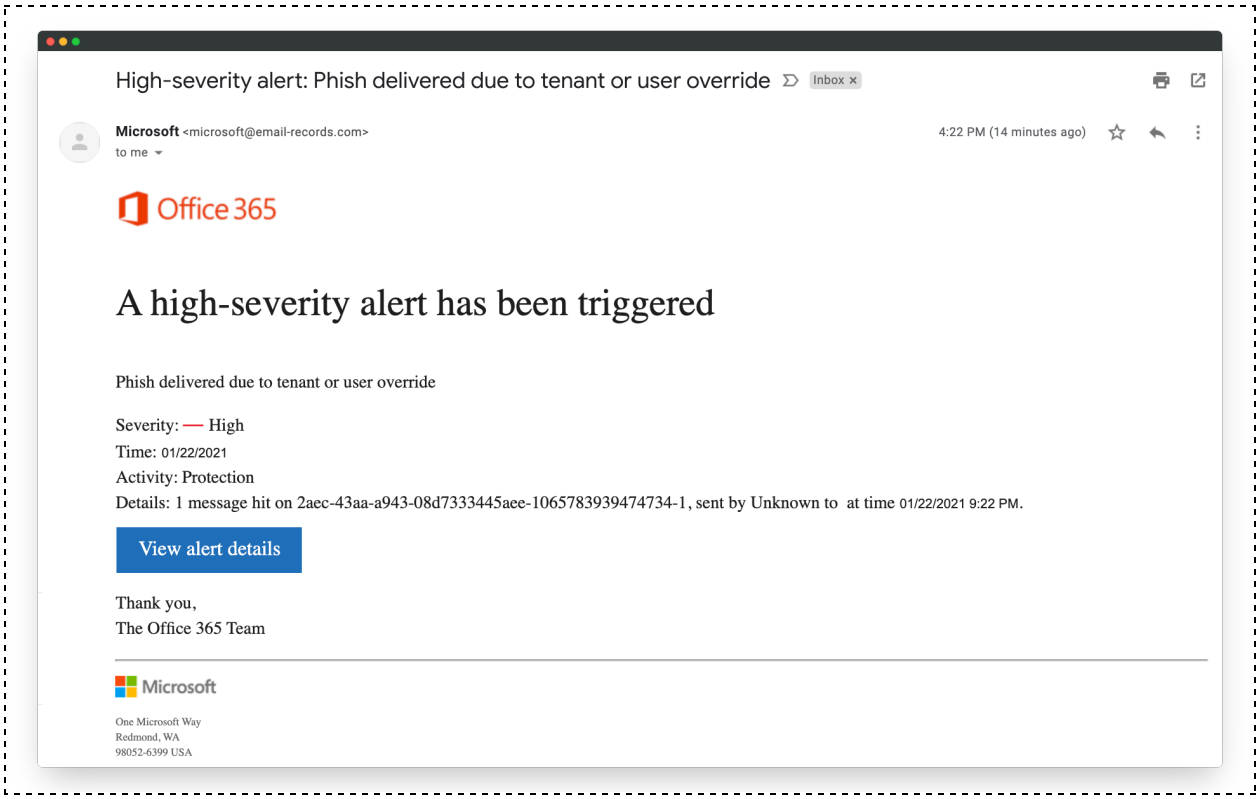
Talk soon,

Jon

PS: You're receiving this email because you requested one of our strategy guides or signed up for emails through BoostBlogTraffic.com. If you no longer want to receive this case study click here to stop getting the emails.

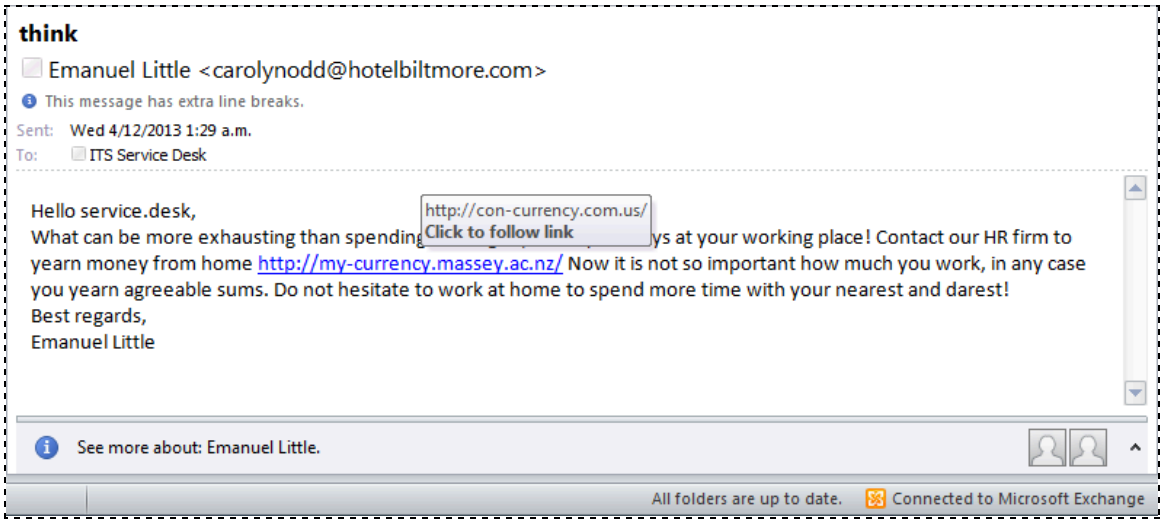
- **Title:** "How to Become a Highly Sought-After Writer (Part 1)"
- **Author:** Jon Morrow
- The email introduces a case study where the author reveals how they wrote an article that attracted over 1 million visitors and led to Forbes approaching them as a columnist.
- It encourages readers to check a previous email titled "Want to be a columnist for a big magazine or newspaper?" for context.
- The author emphasizes breaking down writing techniques, strategy, and traffic generation.
- There's a hyperlink inviting readers to "Click here to read the post."

Case 3:



- **Subject:** “Security alert: Phish delivered due to tenant or user override”
- **Sender:** The email is not from an official Microsoft domain.
- The email claims a “severity alert” has been triggered due to “tenant or user override.”
- It lacks specific details about the incident.
- There’s a hyperlink labeled “View details,” which could be suspicious.

Case 4:


think
Emanuel Little <carolynodd@hotelbiltmore.com>
This message has extra line breaks.
Sent: Wed 4/12/2013 1:29 a.m.
To: ITS Service Desk
Hello service.desk,
What can be more exhausting than spending
http://con-currency.com.us/
Click to follow link
ys at your working place! Contact our HR firm to yearn money from home http://my-currency.massey.ac.nz/ Now it is not so important how much you work, in any case you yearn agreeable sums. Do not hesitate to work at home to spend more time with your nearest and darest!
Best regards,
Emanuel Little
See more about: Emanuel Little.
All folders are up to date.
Connected to Microsoft Exchange

- **Sender:** The email is from an address ending in “@hotelbiltmore.com,” which is not an official Microsoft domain.
- **Hyperlinks:**
    a. “http://con-currency.com.us/”
    b. “my-currency.massey.ac.nz”
- The first link appears suspicious due to its unusual domain structure.
- The second link is embedded within the text.
- **Content:**
    a. The email discusses spending days at work and working from home to spend more time with family.
    b. However, the lack of context and vague information raises suspicion.

Case 5:

Amazon <unexercisable@d505.fzpaunso.us>
to me
Hope you are doing well. I'm writing to you because we want to know if you had a bad experience with our services/website the last time you visited us.
Amazon recognizes the impact of any bad situation in our community. You are worthy member of Amazon community and we will continue to work on improving our services by giving convenience and top notch technology. We are obligated to take steps to protect our beloved customers.
Like our way of saying sorry, please accept this complimentary voucher worth 50 GBP.
CLAIM HERE
Best regards
Sandy S.
Customer Service Representative
amazon.co.uk
Premium

- **Sender:** The email appears to be from “Amazon,” but the sender’s email address is unusual.
- **Content:**
    - The email begins with a friendly greeting and inquires about the recipient’s previous experience with Amazon’s services or website.
    - It emphasizes Amazon’s commitment to community and technology.
    - As an apology, the email offers a “complimentary voucher worth 50 GBP.”
    - The recipient is prompted to “CLAIM HERE” by clicking on an orange button.
    - The closing includes “Kind regards” from “Andy S.,” identified as a Customer Service Representative.
    - Logos for Amazon Premium and amazon.co.uk are visible at the bottom.
- **Phishing Indicators:**

    - Unusual Sender Email: The sender's email address does not match the official Amazon domain.
    - Urgency: The offer of a voucher creates a sense of urgency.
    - Suspicious Link: The "CLAIM HERE" button may lead to a phishing website.
- **Prevention Tips:**
    - Always verify the sender's identity before clicking on any links.
    - Inspect URLs closely to ensure they lead to legitimate websites.
    - Be cautious when receiving unexpected emails, especially those offering rewards or requesting personal information.

Also view at https://sites.google.com/view/owca/notes/02-12-2024